Appendix 4: Technical Architecture for Services: Technical Architecture

Table of Contents

List of Figures

List of Tables

1 Introduction

The American Recovery and Reinvestment Act of 2009 (ARRA), through the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), sets forth a plan for advancing the appropriate use of health information technology (HIT) to improve quality of care and establish a foundation for health care reform. HITECH establishes several new grant programs that will provide resources to promote nationwide use of HIT. Together, they are intended to facilitate the adoption and use of electronic health records (EHRs) by providing technical assistance, the capacity to exchange health information, and the availability of trained professionals to support these activities.

The Office of the National Coordinator for Health Information Technology (ONC) within the Department of Health and Human Services (HHS) serves as the principal federal entity charged with coordinating the overall effort to implement a nationwide HIT infrastructure that allows for the electronic use and exchange of health information. The State Health Information Exchange Cooperative Agreements Program sponsored by ONC is a funding opportunity designed to promote health information exchange (HIE) that will advance mechanisms for information sharing across the health care system. Awards under the program are being made in the form of cooperative agreements to states or qualified state-designated entities (SDEs). The purpose of this program is to continuously improve and expand HIE services over time to reach all health care providers in an effort to improve the quality and efficiency of health care. Cooperative agreement recipients will evolve and advance the necessary governance, policies, technical services, business operations and financing mechanisms for HIE over a four year performance period. ONC envisions that this program will build off of existing efforts to advance regional and state level HIE while moving towards nationwide interoperability.

HITECH and the State HIE Cooperative Agreements Program provides a tremendous opportunity to rapidly accelerate implementation of HIT and advance HIE in California. Careful planning is key to realizing the promises of HITECH. The State, in cooperation with ONC, is developing a set of planning documents to guide development of statewide HIE and use of State resources. Key among them is an Implementation Plan for statewide shared services.

The Operational Plan for California's health information exchange began to describe an architecture for statewide shared services, including a set of potential shared services, divided into so called "core" infrastructure services and so-called "non-core" value-added services. The analysis of requirements and the strategic approach to shared services that supports development of an Implementation Plan adds:

1) functional requirements for statewide exchange based on meaningful use criteria, the Interim Final Rule (IFR) on interoperability standards published by ONC, Nationwide Health Information Network (NHIN) and NHIN Direct standards and services, and State requirements for functionality, privacy, and security;
2) high-level technical requirements for shared services derived from these functional, privacy, security, and standards requirements; and
3) a strategic approach to implementing shared services vetted by stakeholders.

The Technology Strategy for shared services outlined the high-level conceptual approach to developing the core infrastructure for shared services and valued-added shared services. A more detailed analysis of service offerings should incorporate the following analysis:

1) a more detailed architecture design and specification of standards for the core infrastructure components and services;
2) identification of the high-priority business processes to be supported by non-core value-added services;
3) a description of the interactions between core infrastructure components and non-core value-added components; and
4) a strategy for developing the core infrastructure components and non-core value-added services.

This document will summarize a more-detailed, but still high-level, architectural design for statewide shared services as a recommendation for implementation in California, considering the analysis of the meaningful use criteria, the IFR, NHIN standards and services, NHIN Direct standards and services, and State requirements, the strategic approach to shared services, and consensus discussions with stakeholders.

The output of this analysis will, in fact, form the basis for details for a work plan for implementing statewide shared services and resource allocation by defining the technical and business offerings that Cal eConnect and the statewide HIE will "offer" the community of potential users. Therefore, this analysis is an important component of the overall Implementation Plan.

1.1 Scope of the Analysis

The overall goal of the set of documents that outline the Technical Architecture for Services is to define Cal eConnect's technical solution for statewide HIE. They describe the technical architecture, and the detailed plan for implementing the architecture and operating and maintaining the components and services it supports.

This document, Technical Architecture, is the second among the document set, and a description of the technical system-level architecture for statewide shared services. For each component in the architecture, it outlines a procurement strategy and staffing requirements. This analysis will inform the development of a detailed implementation and operational plan for shared services.

The architecture for a system is its structure, comprising software elements, the externally-visible properties of those elements, and the relationship among them. The concept of "externally visible" is meant to identify the assumptions developers and the software elements they create can make of an element that is part of the architecture. Those assumptions might include the services the element provides, performance characteristics, fault handling, shared resource usage, and so on.

This definition provides the basic litmus test for what information is included in this document. Software design information for the internal workings of software elements often finds its way into architecture documentation. This document attempts to incorporate only architectural information at the system level.

- *Elements and relationships*. The system architecture first and foremost embodies information about how software elements relate to each other. This means that this document specifically omits details to interactions. Elements interact with each other by means of interfaces that are partitioned into public and private parts. Architecture is concerned with the public side of this division.

- *Architectural views*. Systems can, and often do, comprise a complex structure best illuminated by considering differing perspectives that illustrate different properties. Therefore, architectures are often document through various so-called "views" of the architecture. A more complete architecture document might include various views conforming to Universal Modeling Language (UML) standards. This document describes the architecture primarily through component diagrams and descriptions of the characteristics of the components within them.
- *Behavior*. Although architecture tends to focus on structural information, behavior of each element is part of the architecture insofar as that behavior can be observed or discerned from the point of view of another element. This behavior is what allows elements to interact with each other, which is clearly part of the software architecture and will be documented here as such. This document describes behavior through sequence diagrams.

1.2 Methodology

The architecture for statewide shared services was developed based on an analysis of meaningful use requirements, security and privacy requirements, and nationwide standards that produced a technology strategy outlined in:

1) *Technical Architecture for Services – Technology Strategy*, a document that accompanies this Technical Architecture document as part of a set of deliverables supporting the development of an Implementation Plan for statewide exchange supported by the State HIE Cooperative Agreement Program.

In addition, the California Health and Human Services Agency (CHHS) established the California eHealth Technical Advisory Committee and Technical Working Group as consensus organizations to establish a technical strategy for shared services that might be developed under the State HIE Cooperative Agreement Program. Much of the information from the deliberations of these organizations form the basis for the Technology Strategy and this Technical Architecture. A discussion of that strategy can be found in:

1) "California Health Information Exchange Strategic and Operational Plans" published by CHHS on 31 March 2010, which can be downloaded from http://www.ehealth.ca.gov/LinkClick.aspx?fileticket=zK7zQxE20no%3d&tabid=72.

The analysis for the Technology Strategy and this Technical Architecture was also based on a set of documents published by the federal government that describe nationwide standards for interoperability. They include:

2) "Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Interim Final Rule" published by the Department of Health and Human Services in the Federal Register on 13 January 2010, 45 CFR Part 170, which can be downloaded from http://edocket.access.gpo.gov/2010/pdf/E9-31216.pdf.
3) The 2010 Final Production Specifications for the Nationwide Health Information Network provisionally approved by the NHIN Technical Committee and subject to the validation of the NHIN reference implementation, all available on the NHIN section of the HHS web site at http://healthit.hhs.gov (search for NHIN Exchange).
4) Material on the NHIN Direct wiki at http://nhindirect.org/.

1.2.1 Requirements Analysis

This document does not include a detailed requirements analysis. That analysis is instead included in the Technology Strategy document that accompanies it. The following is simply a summary of those findings.

On 13 January 2010, the Center for Medicare and Medicaid Services (CMS) published a draft rule to implement the meaningful use provisions of ARRA, including the criteria for provider to quality for meaningful use incentives. The State HIE Cooperative Agreement Program in turn calls for activities that are consistent with and support providers in qualifying for meaningful use incentives. Therefore, the criteria for meaningful use are an important defining component of the functional requirements in developing statewide exchange.

The draft rule calls out 25 criteria for meaningful use of EHR technology. Of these, 13 have been identified as requiring HIE or significantly benefiting from HIE:

1) Use e-prescribing where permissible
2) Incorporate structured lab results
3) Check eligibility electronically
4) Submit claims electronically
5) Provide patients with an electronic copy of their health information
6) Provide patients with online access
7) Exchange information among patient-authorized providers or entities
8) Provide summary of care for transitions and referrals
9) Submit data to immunization registries
10) Submit lab results to public health
11) Submit surveillance data to public health
12) Report aggregated quality data to CMS
13) Perform medication reconciliation

In addition, the meaningful use criteria also require security risk analysis be performed on all HIT initiatives.

An analysis of the 13 criteria identified a set standards-based technical and service specifications and a set of software components that are required to support meaningful use that either require or can benefit from HIE. Table 1 and Table 2 below summarize the required technical specifications and software components, respectively.

Table 1 Summary of required technical specifications derived from meaningful use criteria.

1	a standards-based message framework for secure and reliable health information exchange
2	a trust framework for authorization and consumer consent
3	a standards-based service interface to a root certificate authority that “authenticates” an entity
4	a standards-based service interface to a directory of all entities participating in exchange
5	a standards-based service interface to a directory of providers participating in exchange

6	a standards-based service specification for discovering patient identities and agree on shared identities
7	a standards-based service specification for (1) a push exchange pattern, (2) a query and response exchange pattern, and (3) a publish and subscribe exchange pattern

Table 2 Summary of required key software components derived from meaningful use criteria.

1	a digital certificate authority that is supported by a standards-based interface and supporting the messaging framework and trust framework
2	a directory of entities participating in exchange, including provider organizations of various sizes, chain and independent pharmacies, labs, public and private health plans, other patient authorized entities such as PHRs or patient-controlled health records (PCHRs), and public health departments and systems, supported by a standards-based interface and supporting the messaging framework
3	a directory of providers participating in exchange, which might be centralized or federated and is supported by a standards-based interface
4	a gateway interface to the Nationwide Health Information Network

Many of the specifications in Table 1 and software components in Table 2 are included in specifications and infrastructure components of NHIN Exchange, and might be used to inform development of these capabilities for the State. Conspicuously missing, however, is any mechanism for locating providers.

1.2.2 Technology Strategy

The overall technology strategy for statewide services to support meaningful use includes the following key components:

1) The strategy is based on a service-oriented approach to system design using the Internet.
2) The strategy includes the development of technical specifications and software components required for meaningful use as outlined in Table 1.
3) The software components included in the strategy may be separated into:
   a) infrastructure components that establish trust through secure, encrypted, and reliable exchange of health information over the Internet, and
   b) optional value-added services that enable higher-level business processes.
4) Policy must inform the development of the messaging framework and trust framework specifications.

5) The infrastructure components implement the messaging framework and trust framework specifications.
6) The messaging and trust framework for the statewide exchange must be consistent with the transport standards and security standards identified in the IFR.
7) The services and standards developed for NHIN Exchange should inform the development of the statewide infrastructure and be utilized or leveraged where possible.

The technical architecture described in this document is based on this technology strategy.

2 Architecture Overview

The statewide architecture for shared services is divided into three areas:

- *State Infrastructure* is a minimal set of technical resources that enable statewide exchange, including the key standards-based specifications for the messaging framework and trust framework and software components that provide entity and provider directory services. The Infrastructure establishes a secure and reliable basis for health information exchange compliant with State policy and enabling meaningful use.
- *Discovery and Exchange Service Specifications* form the technical interface details for a set of standards-based mechanisms that can be used by organizations to locate and exchange information on a statewide basis. The use of these service specifications may be optional or required, based on State policy yet to be determined.
- *Business Services* that provide an expanding set of value-added software services that enable higher-level business processes. While not required by meaningful use, Business Services provide the heavy lifting that reduce the burden on organizations in exchanging data and realizing value in achieving meaningful use.

The following sections follow this structure in describing the architecture.

2.1 Definitions

A small set of definitions help one understand the technology strategy for statewide shared services, and describe the elements included in the proposed high-level system architecture and how they may interact. Certain definitions are based on ONC consensus definitions, whereas others are *ad hoc* definitions intended specifically to explain the architecture described here.

- *Entity*: A legal business entity that assumes responsibility for safeguarding the patient health information under its control and for managing in a secure manner the exchange of protected health information (PHI). Entities may be physician practices, hospitals, clinics, pharmacies, health plans, state or federal agencies, IDNs, health systems, HIOs, or other organizations. The responsibilities of Entities include ensuring that their users are reliably authenticated when they request access to PHI that is controlled by other entities, and reliably authorizing access to the PHI they control when requested by other Entities.
- *HIO*: Or health information organization, an organization that oversees and governs the exchange of health-related information among principals. HIOs may include regional

HIOs, IPAs, or other private non-profit, private for-profit, or government entities that oversee and govern HIE. An HIO is an Entity.

- *Node*: A health IT system that exists on the Internet and implements services that participate in statewide HIE in accordance with the messaging framework and authorization framework. Nodes may include EHRs, practice management (PM) systems, lab information systems (LISs), immunization registries, public health reporting and surveillance data warehouses, personal health records (PHRs) or patient-controlled health records (PCHRs), health plan claims and eligibility systems, etc. Nodes are not equivalent to Entities, but are operated by them. Entities take responsibility for Nodes.
- *State Infrastructure*: Or Infrastructure, a minimal set of technical resources that enable statewide HIE, including the key standards-based specifications for the messaging framework and trust framework and software components that provide entity and provider directory services. Together, the resources of the Infrastructure establish a secure and reliable basis for health information exchange compliant with State policy and enabling meaningful use; managed, overseen, regulated and/or financially supported to some extent by Cal eConnect.
- *Business Services*: A set of optional value-added software components and their service-oriented interfaces available to any eligible stakeholder in the California health care system, built upon and using the State Infrastructure in order to enable value-added business processes; Business Services may be governed, developed, and operated by Cal eConnect, or may be developed, operated, and offered by third parties under Cal eConnect governance.

A larger set of definitions is included in the Operational Plan, but are not necessary for this discussion.

2.2 Example Illustrating Portions of the Architecture

Figure 1 illustrates how stakeholder Entities, HIOs, and providers or other users within them make use of the State Infrastructure and Business Services to exchange health information.

In this illustration, a lab (an Entity) wishes to use its lab information system (LIS) (a Node) to send a structured lab result to the EHR (another Node within another Entity, perhaps an HIO) used by a specific provider identified in the lab order. To do this, it:

1) uses directory services of the State Infrastructure to identify a web service address for the recipient provider's EHR and a definition of the protocol used to send information to it;
2) uses certificate services of the State Infrastructure to create a secure, encrypted, and validated connection to the EHR; and
3) uses a standards-based service to exchange the information; perhaps one identified by a mandatory Exchange Service Specification.

In order to achieve this exchange, the lab system takes responsibility for creating structured lab result content. The State takes responsibility for supporting the lab in locating the provider's EHR on the network and facilitating a secure, encrypted, reliable connection to that and only that EHR. The provider's HIO or EHR vendor takes responsibility for incorporating the structured lab result content into the EHR.

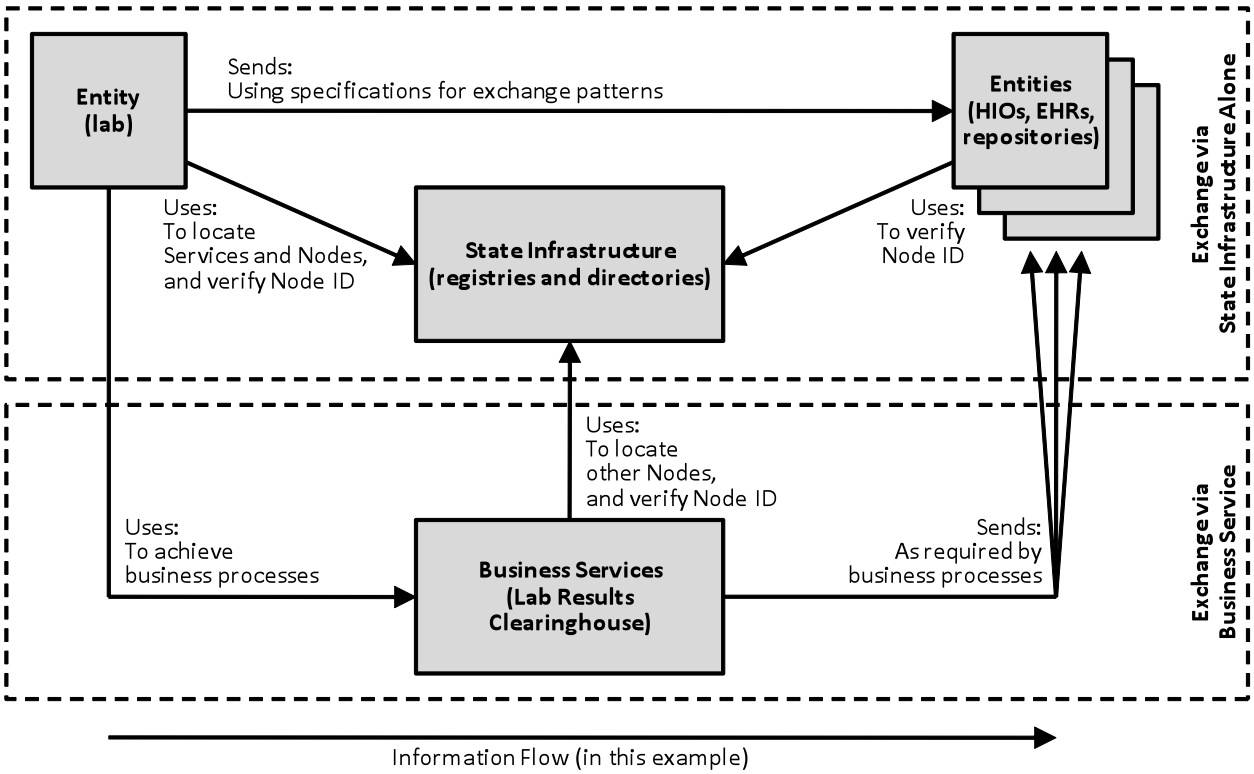

Figure 1 High-level view of the interactions between stakeholders, the State Infrastructure for shared services, and Business Services.

Alternatively, the lab could send a structured lab result to a clearinghouse (Business Service) along with intended recipients of that result, such as the ordering specialist and primary care provider. To this, the lab:

1) uses directory services of the State Infrastructure to identify a web service address for the clearinghouse Business Service and a definition of the protocol used to send information to it;
2) uses certificate services of the State Infrastructure to create a secure, encrypted, and validated connection to the clearinghouse; and
3) uses a standards-based service to exchange the information; perhaps one identified by a mandatory Exchange Service Specification or perhaps one specific to the Business Service.

The clearinghouse in turn:

4) uses directory services of the State Infrastructure to identify a web service address for the specialist provider's EHR and the primary care physician's EHR, and definitions of the protocols used to send information to them, which may be different;
5) determines whether the result is to be reported to public health, and if so, uses directory services of the State Infrastructure to identify a web service address the public health reporting system and a definition of the protocol used to send information to it;

6) translates the structured lab result into the terminology used by each system and transforms the format into the standard used by each system, again all of which may be different;
7) removes identifying information from the message bound for the public health system, if required;
8) uses certificate services of the State Infrastructure to create secure, encrypted, and validated connections to both EHRs and the public health system in turn; and
9) uses standards-based services to exchange the information with each system, in turn; perhaps using services identified by mandatory Exchange Service Specification.

While the process utilized by the Business Service is clearly more complex, it also illustrates how the burden on the lab and its LIM can be relieved using Business Services. In order to achieve this exchange, the lab system still takes responsibility for creating structured lab result content. The Business Service orchestrates the complex business process for lab results delivery. The State takes responsibility for supporting the Business Service in locating the providers' EHRs and public health system on the network and facilitating secure, encrypted, reliable connections. The providers' HIO or EHR vendors and public health agency take responsibility for incorporating the structured lab result content into the EHRs and public health systems, respectively.

3 State Infrastructure

The State Infrastructure, or simply Infrastructure, is a minimal set of technical resources that enable statewide exchange. It establishes a secure and reliable basis for health information exchange that is compliant with State policy and enabling meaningful use. The State Infrastructure is managed, overseen, regulated and/or financially supported to some extent by Cal eConnect.

The State Infrastructure comprises two specifications that establish the framework for secure web services and patient consent using service-oriented design. The specifications comprise:

- *Messaging Framework*: Specifications for the basic exchange of information over the Internet. The Messaging Framework is based on web services following recognized national standards. It includes specifications for the web service standards, acceptable encryption standards, and the use of digital certificates to establish secure and reliable encrypted exchange.
- *Authorization Framework*: Specifications for how Entities assert authorization for information requests, and how those assertions are carried within the Messaging Framework. The Authorization Framework must identify how the key requirements of CalPSAB authorization and access controls are addressed, including how to represent the data source, entity of requestor, role of requestor, use of data, sensitivity of data, and consent directives of the data subject are addressed. The Authorization Framework must enable both State and NHIN policies associated with patient consent.

It also includes two software components and web service interface specifications that may be used to access information they maintain. These components comprise:

- *Entity Registry*: The a trusted registry of Entities engaged in statewide exchange and the Nodes or systems for which they are responsible. The Registry serves to ensure parties

engaged in exchange of the validity and authenticity of exchange partners. It also provides the primary control point for the State to enforce policies associated with health information exchange. Only Entities and Nodes with valid entries in the Entity Registry can exchange information using the State Infrastructure.

- *Service Registry*: The Service Registry provides information about how and where to direct information intended for specific individuals or systems, such a providers or their specific EHRs, and how to formulate the transactions such that they can be correctly processed when received.

3.1 Messaging and Authorization Framework

Key to a trust framework is developing a standards-based framework for messaging and authorization for the exchange of information. The Messaging Framework and Authorization Framework comprise two documents that establish the standards and patterns used to trust.

3.1.1 Messaging Framework Specification

The Messaging Framework comprises a technical specification for web services-based health information exchange over the Internet. It incorporates the security requirements for exchange of protected health information (PHI), and therefore should be used primarily for that purpose, and not for the exchange of public information.

The Message Framework should be based on:

1) SOAP[1] version 1.2, a protocol specification developed and maintained by the World Wide Web Consortium (W3C) for exchanging structured information web services that relies on eXtensible Markup Language (XML) as its message format ; and
2) Hypertext Transport Protocol (HTTP) version 1.1, an protocol used by the World Wide Web for message negotiation and transmission.

   SOAP and HTTP, as well as a number of related standards that might be used in the Messaging Framework, are taken from the Web Services Interoperability (WS-I) industry consortium WS-I Basic Profile for web services.

   There are alternatives to this structure, most notably the use of Representational State Transfer (REST) web services over HTTP rather than SOAP.
3) HTTP using two-way encryption based on the Transport Layer Security (TLS) version 2 cryptographic protocol to provide security for communications over the Internet;
4) encryption and decryption of electronic health information is based on AES standard adopted by the U.S. government;
5) Transport is to be over and the Internet Protocol Security (IPsec) protocol suite for securing communications by authenticating and encrypting each packet of a data stream;

[1] SOAP was originally defined as the Simple Object Access Protocol, but the acronym was dropped with version 1.2 of the standard.

6) Secure Hash Algorithm-1 (SHA-1), a cryptographic hash function designed by the National Security Agency (NSA), to ensure that information is not altered or corrupted during transmission; and

7) Use of X.509 digital certificates for verifying Node identity, establishing two-way encryption, and hash algorithm validation of unaltered transmission.

   Use of TLS, AES, IPsec, SHA-1, and X-509 certificates, as well as a number of related security standards, are taken from the WS-I Basic Security Profile for web services, to establish secure and reliable health information exchange.

This approach to the Messaging Framework is compliant with the Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Interim Final Rule published by HHS and ONC.

The completed Message Framework specification outlines the details of how the above standards are used within the statewide exchange, and is established and managed through a transparent and structured process.

3.1.2 Authorization Framework Specification

Authorization for the exchange of information is based on the concept of local autonomy – each Entity participating in exchange makes its own independent decisions on whether to provide the requested information. Those decisions are based on national and State legal and regulatory requirements, data use agreements established by the State for statewide exchange, local organizational policy and stakeholder needs, and local patient consent for exchange. In particular, the management of patient consent is established locally using local procedures, but in compliance with State guidelines.

This approach to authorization is likewise supported by the IFR and by NHIN specifications. It is reinforced by the Data Use and Reciprocal Service Agreement (DURSA) that comprises the data use agreement among NHIN participants.

The Authorization Framework specifies the details of the information that accompanies health information to enable this process. Every request for and exchange of information is accompanied by:

1) the identity of the requestor in plain text and accompanying National Provider Identifier (NPI) and role of the requestor from the HL7 specification of potential roles;

2) the requestor's Entity as an Object Identifier (OID) following the HL7 standards for unique identifiers and issued by HL7;

3) the purpose-for-use of the request from the HL7 specification of potential uses, and sensitivity of the data exchange; and

4) the unique and unambiguous identifier for the target patient for the request or exchange in both organizations conducting the exchange.

This information is carried in a Security Assertion Markup Language (SAML) assertion –an XML-based standard for exchanging authentication and authorization data – encapsulated within every SOAP message that comprises a portion of the exchange. The SAML assertion is signed using a X.509 digital certificate by the Entity making the request, and therefore forms a verified assertion of the authority of the individual by that Entity. The organization that receives the request examines the role and purpose-for-use and Entity identifying information, makes a log of the request, and releases the information if and only if it conforms with its own local policy

for disclosure of health information. The policy check would normally include a check of the consent preferences of patients as known to the local entity.

Figure 2 below illustrates authorization and patient consent works within the State Infrastructure specified in the Authorization Framework.

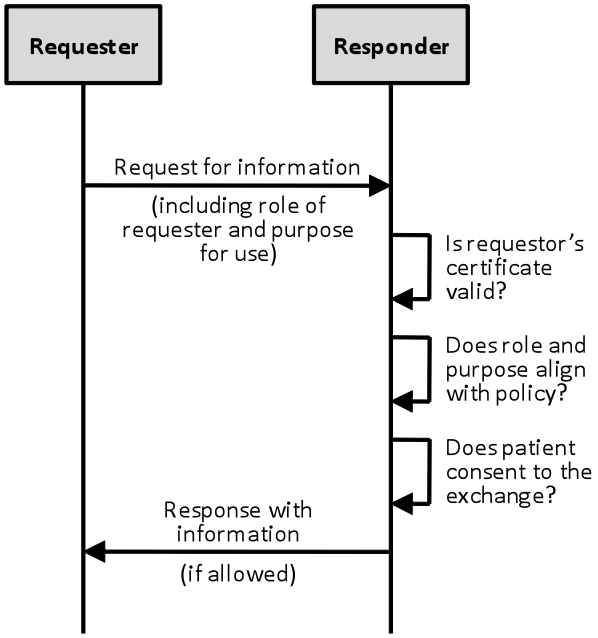

Figure 2 Illustration of the Authorization Framework and the concept of local autonomy.

Like the Message Framework specification, the completed Authorization Framework specification outlines the details of how the above standards are used within the statewide exchange, including the roles and purpose-for-use that may be specified, and how the identity of the individual making the request and the organization to which he/she belongs are represented.

The Messaging Framework and Authorization Framework do not require any centralized patient consent registry or uniform policy for the disclosure of health information. Instead, the State Infrastructure is dependent upon local policy of the disclosing organization, and patient preferences for consent known to and managed by that organization. This approach allows autonomous organizations to implement disclosure policies that meet the needs of their stakeholders. It also allows patients to consent to disclosure using different rules depending upon the sensitivity of the information present within different organizations, and manage those rules at the point of care as needed.

3.1.3 Digital Certificate Authority

The Messaging Framework and Authorization Framework both require a secure, centralized, and authoritative certificate authority that stores

1) digital certificates of Nodes that are used in

a) validating that the Nodes are in fact the systems they claim to be, based on third-party verification,

b) establishing a secure and encrypted connection for exchange of the Internet, and

c) ensuring that the information arrives uncorrupted and unaltered at its destination; and

2) digital certificates of Entities that are used to validate the SAML assertions of authorization for the exchange.

This capability is included in the Entity Registry described in Section 3.2.

3.1.4 Implementation Strategy

Cal eConnect should take responsibility for developing the specifications for the Messaging Framework and Authorization Framework, as the governance entity for the statewide exchange and manager of the State Infrastructure. The above discussion outlines the basic standards and behavior dictated by the Messaging Framework and Authorization Framework. Details of the specification should be defined through an open and transparent process that includes stakeholders throughout the State.

The development of these specifications must be preceded by definition of the policies that define privacy and security, and the role and process for patient consent.

There exist several models for standards development, including perhaps those of the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), and IHE. An analysis of the commonalities among these three recommends a set of best practices that include:

1) An open, inclusive process including input from a board industry cross-section, not only for public comment, but likewise for the drafting of new specifications.

2) A controlled, transparent mechanism for prioritizing development of new specifications and advancing them through the development process.

3) A managed and documented model for the maturity of a developing specification that defines the roles of all participants at each stage of development.

4) A process to subject specifications to implementation testing to assess whether a specification is complete and can be implemented.

Cal eConnect should take responsibility for defining the process for defining, testing, and maintaining specifications, and convening the organizations responsible for implementing that process.

3.1.5 Resource Requirements

The model for the Messaging Framework and Authorization Framework are based on those of NHIN Exchange and are compliant with ONC requirements for standards and certification identified in the IFR. As such, it should be possible to complete this action through a minimal technical staff working in conjunction with working groups comprising volunteers from the stakeholder community and in a short period of time.

Specifications development should be managed part time by a CTO or Systems Architect on staff with Cal eConnect (perhaps 20% effort) over a 2-month period, utilizing one full-time staff facilitator and one full-time technical writer or consultant to manage workgroup(s) , draft the

specifications, and review public comments. The workgroups in turn comprise volunteers from the community.

The process will require the use of web sites to publish drafts and collect comments (perhaps using a wiki or other Web 2.0 mechanism), and web-based meetings to facilitate the workgroups.

3.2 Entity Registry

The Entity Registry contains listings of the Entities and Nodes that are participating in exchange, along with a unique identifier and a digital certificate for each. Digital certificates associated with Entities are used to sign assertions of authorizations in compliance with the Authorization Framework. Digital certificates associated with Nodes are used to establish secure, encrypted connections with other Nodes in compliance with the Messaging Framework, validating the identify of each Node, and ensuring that exchange is completed without corruption or alteration.

The Entity Registry therefore comprises:

1) a store for Entity and Node information and the digital certificates associated with them, and
2) standards-based interfaces to that store.

The Entity Registry is similar in structure and function to the certificate authority of NHIN Exchange, although unlike NHIN, it provides for Entities and Nodes to each have their own certificates. In the NHIN paradigm, Nodes sign authorizations on behalf of the Entity and there is no separation between the certificates associated with encrypted connections and certificates used to authorize exchange. This limitation has proven an issue when multiple Entities share a Node, or perhaps when a single Entity has multiple Nodes.

The Entity Registry conforms to X.509 standards for the storage, retrieval, and revocation of digital certificates. Its store includes the plain-text name of the Entity or Node, a unique identifier based on an HL7 OID, and sufficient information about the location and type of Entity or Node to allow a search of the Registry to retrieve appropriate Entities and Nodes. The completed specification for the Entity Registry service interface outlines the details of how these standards are used within the statewide exchange, and is established and managed through a transparent and structured process.

Figure 3 provides a high-level architecture view of the Entity Registry, comprising a single central and authoritative repository for public digital certificates.

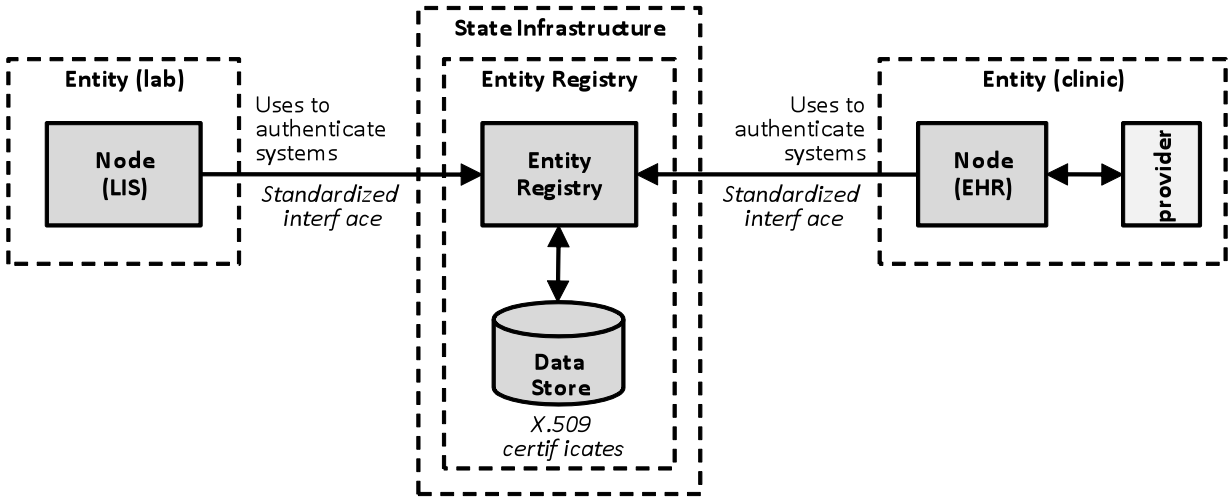

Figure 3 High-level architectural view of the Entity Registry.

The data store associated with the Entity Registry contains information about the Entities and Nodes, as well as the digital certificates associated with them.

3.2.1 Implementation Strategy

Cal eConnect should take responsibility for developing the specifications for and operating the Entity Registry, as the governance entity for the statewide exchange and manager of the State Infrastructure.

The Entity Registry is the primary enforcement point for compliance with State policies and agreements. No Entity or Node can participate in an exchange unless it has an entry and valid digital certificate in the Entity Registry. Therefore, Cal eConnect should develop rigorous processes for provisioning and monitoring organizational compliance with its policies, mechanisms for addressing complaints by stakeholders, and a rapid process for certificate revocation to ensure that trust in the State Infrastructure is not compromised.

The above discussion outlines the basic standards and behavior of the Entity Registry. Details of the specification for the Registry and its interfaces should be defined through an open and transparent process that includes stakeholders throughout the State, similar to that outlined for the Messaging Framework and Authorization Framework.

The Entity Registry conforms to the Messaging Framework specification, and therefore must be defined in detail after the Messaging Framework is complete.

The Entity Registry is based on well-established industry standards for certificate repositories. A technical solution is available from several vendors. The Entity Registry therefore should be procured through a competitive process

a) as a solution to be operated by Cal eConnect, or
b) as a service provided to Cal eConnect through a software-as-a-service (SaaS) or similar business model, but under Cal eConnect governance.

3.2.2 Resource Requirements

The model for the Entity Registry is based on industry standards and is compliant with ONC requirements for standards and certification identified in the IFR. As such, it should be possible to complete the development of the Entity Registry specification through a minimal technical staff working with volunteers from the stakeholder community – much like the specifications for the Messaging Framework and Authorization Framework.

Specifications development should be managed part time by a CTO or Systems Architect on staff with Cal eConnect (perhaps 20% effort) over a 2-month period following completion of the Messaging Framework specification, utilizing one full-time staff facilitator and one full-time technical writer or consultant to manage the workgroup, draft the specifications, and review public comments.

The process will require the use of web sites to publish drafts and collect comments (perhaps using a wiki or other Web 2.0 mechanism), and web-based meetings to facilitate the workgroups.

The procurement will require a consultant to draft the RFP under the oversight of a CTO over the course of two months, including approval by Cal eConnect, one month to answer questions on the RFP and collect responses, and two months to review and award a contract. The review process should likewise be overseen by the CTO, and include perhaps six other reviewers selected to provide wide stakeholder representation.

It should be possible to implement the Entity Registry within three months, with oversight by the CTO part-time, and management by a full-time project manager.

3.3 Service Registry

The Service Registry contains mappings between individuals or network resources (services or systems) and web service addresses and protocols. It is the primary directory that Nodes use to locate recipients of health information or systems from which to request health information.

Logically, the Service Registry therefore comprises:

1) a store for providers, physician practices, hospitals, hospital departments, laboratories, pharmacies, personal health records, immunization registries, payers, and any other resources to whom health information could be legitimately sent or from whom health information could be requested, along with information such as location, type of resource, type of information exchange supported, etc, that can be used to locate it in a search; and
2) standards-based interfaces to that store.

A search for an entry in the Service Registry returns web service information, such as the Entity and Node identifiers used in the Entity Registry, a web service address to be used in accessing the service, and the protocol to use.

Physically, the Service Registry is a federated store. That is, “local” Service Registries may exist at individual Entities that are managed by those Entities, in addition to a “central” Service Registry operated by the State for those Entities that do not wish to operate one themselves. A component of the central Service Registry is an interface that, if used, performs a search of the information on all Service Registries, including all local Registries. It therefore appears to be a “global” Service Registry. Using this approach, a user of the global Service Registry need not know the Entity associated with a provider or other network resource in order to locate it.

However, it still provides a mechanism for individual Entities to manage the information associated with their systems and users, including identifying information of individual providers. It also allows a Node to contact a local Entity Registry directly if the Entity and location of the local Entity Registry service address is in fact known.

The Service Registry conforms to the Uniform Universal Description, Discovery and Integration (UDDI) XML-based registry standard for Internet service directories. UDDI is an open industry initiative enabling Entities to publish services and discover each other and define how the services or software applications interact over the Internet. A UDDI entry includes “White Pages” that include address, contact, and known identifiers, “Yellow Pages” for industrial categorizations based on standard taxonomies, and “Green Pages” with technical information about services exposed by the Entity. UDDI is a core web service standard designed to be interrogated by SOAP messages and to provide access to Web Services Description Language (WSDL) documents describing the protocol bindings and message formats required to interact with the web services listed in its directory. All local and global Service Registries communicate via the UDDI standard. The global Service Registry may cache local Service Registry information to improve the service level and response time. Nodes may likewise cache Service Registry information, as the UDDI specification includes a time-to-live provision that estimates the time for which a cached value may be assumed to be valid.

The Service Registry supports the Messaging Framework by providing the web service address locations and protocols necessary to establish connections.

Figure 4 provides a high-level architecture view of the federated Service Registry, comprising a single global Service Registry with an orchestrating service that performs federated searches, and multiple local Service Registries.

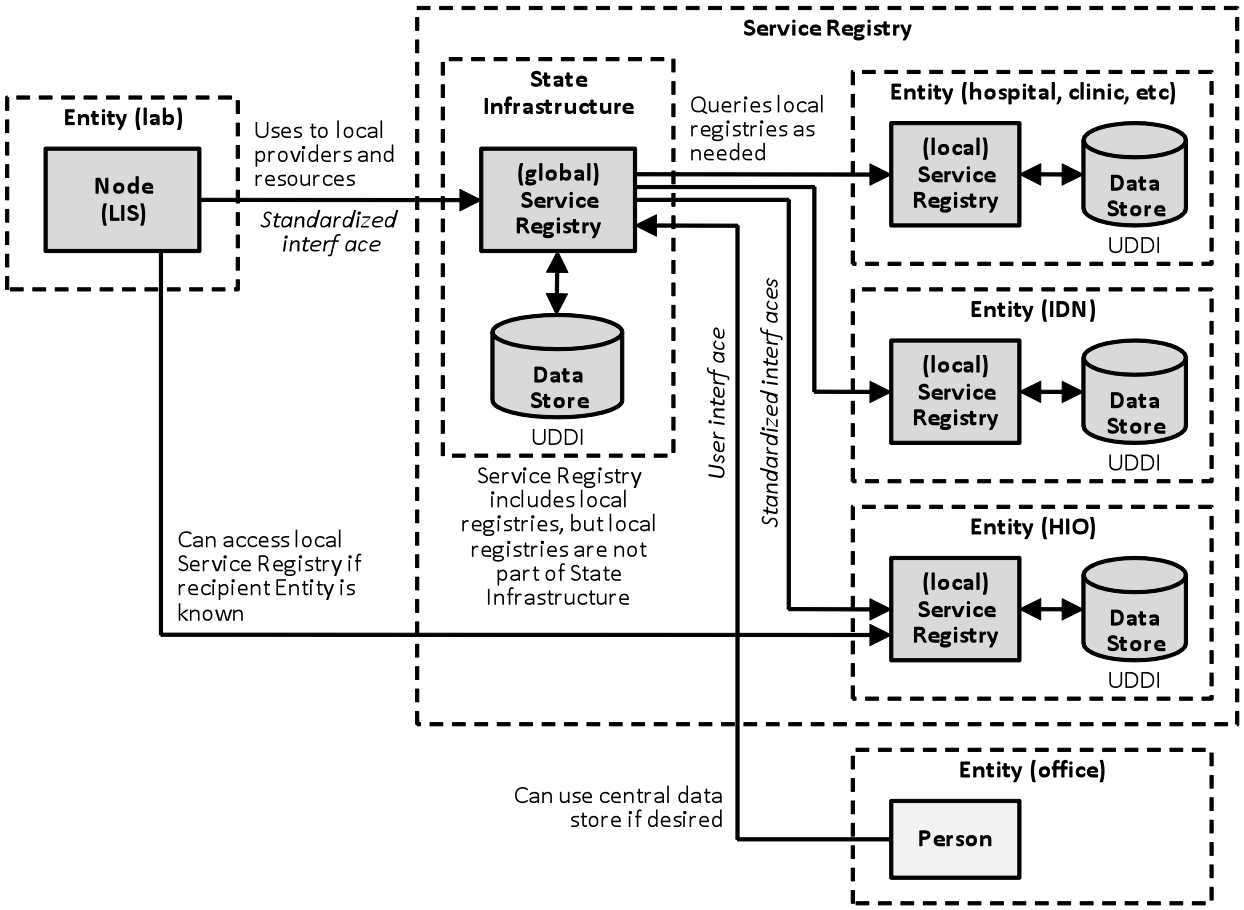

Figure 4 High-level architectural view of the Service Registry.

Within Figure 4, the "(global) Service Registry" is the external view of the Service Registry within the State Infrastructure, and responds to requests statewide[2]. It maintains a UDDI-compliant programmatic interface the federated data store, and maintains a UDDI-compliant partial data store for those Entities that do not wish to maintain their own "(local) Service Registry". The "(local) Service Registry" conforms to the same programmatic interface as the "(global) Service Registry", but is managed locally by an Entity using its own processes and procedures.

3.3.1 Implementation Strategy

Cal eConnect should take responsibility for developing the specifications for and operating the centralized portion of the federated Service Registry (the global Service Registry in Figure 4), as the governance entity for the statewide exchange and manager of the State Infrastructure. Cal eConnect should develop rigorous policies and processes guidelines that stakeholders will use

[2] "Global" in this context refers to globally responding for all state Entities. It does not necessarily require a larger geographic scope, such as responding nationwide.

in provisioning their respective service registries, and for and monitoring organizational compliance with its policies, and mechanisms for addressing complaints by stakeholders.

The above discussion outlines the basic standards and behavior of the service that supports the Service Registry. Details of the specification for the interactions between local Service Registries and the central service, and between the central service and service users should be defined through an open and transparent process that includes stakeholders throughout the State, similar to that outlined for the Messaging Framework and Authorization Framework.

The Service Registry conforms to the Messaging Framework and Authorization Framework specifications, and the specification for it therefore must be defined in detail after the Messaging Framework and Authorization Framework are complete. It references Entities and Nodes in the Entity Registry, and there format must be defined before the specification for the Service Registry can be completed.

The Service Registry is based on well-established industry standards. While similar to the NHIN service registry, the Service Registry goes far beyond its capabilities and therefore has a more complex information model to represent its entries. Likewise, its organization as a federated repository is not common. Technical solutions for a federated UDDI service registry has been proposed using several methods, and an update to the UDDI specification has recently been made specifically to address registry federation. Several vendors and systems integrators have experience in developing UDDI registries and should have the capability to develop a federated solution.

The global Service Registry should be procured through a competitive procurement as a solution to be operated by Cal eConnect or a SaaS service provided to and governed by Cal eConnect. The specification for the Service Registry must define the external interfaces to local Service Registries. However, the implementation of local Service Registries are the responsibility of Entities that desire them, not Cal eConnect. Cal eConnect may wish to support the development of local Service Registries through grants to HIOs or other organizations.

3.3.2 Resource Requirements

The model for the Service Registry is based on industry standards and is compliant with ONC requirements for standards and certification identified in the IFR. However, the Service Registry constitutes a more complex component than the Entity Registry due to the need for it to be federated. Sufficient time must be allocated to develop the full design and specification for the service and registry.

It should be possible to complete the development of the Service Registry specification through a small technical staff working with volunteers from the stakeholder community – somewhat more robust that that for the Entity Registry. Specifications development should be managed part time by a CTO on staff with Cal eConnect (perhaps 50% effort) over a 4-month period following completion of the Authorization Framework specification, utilizing one full-time system architect on staff with Cal eConnect or retained as a consultant, one full-time staff facilitator, and one full-time technical writer or consultant to manage the workgroup, draft the specifications, and review public comments.

The process will require the use of web sites to publish drafts and collect comments (perhaps using a wiki or other Web 2.0 mechanism), and web-based meetings to facilitate the workgroups.

The procurement will require a consultant to draft the RFP under the oversight of a CTO and with advise from the system architect over the course of two months, including approval by Cal eConnect, one month to answer questions on the RFP and collect responses, and two months to review and award a contract. The review process should likewise be overseen by the CTO, and include perhaps six other reviewers selected to provide wide stakeholder representation plus the system architect involved in developing the specification and RFP.

Implementation should be accomplished within six months, with oversight by the CTO part-time, and management by a full-time project manager and half-time security specialist.

Due to the federated nature of the Service Registry, the specification should be published as soon as possible. Individual organizations that do not wish to use the centralized registry storage operated by the State can develop their local Service Registries in parallel with the procurement process for the centralized service. It should be expected that some local Service Registries can come on line prior to completion of the centralized repository and service procured by the State, providing some initial capabilities for the State Infrastructure prior to full operational capacity of the Service Registry.

3.4 Summary

Table 3 below summarizes the traceability between the standards-based specifications and core software components and the requirements of meaningful use listed in Table 1 and Table 2.

Table 3 Traceability illustrating how the infrastructure components fulfill the technical requirements of the meaningful use criteria that require or benefit from HIE.

Meaningful Use Requirement	Infrastructure Component
a standards-based message framework for secure and reliable exchange	*Messaging Framework*
a trust framework for authorization and consumer consent	*Trust Framework*
a standards-based interface to a root certificate authority that “authenticates” an entity or individual	*Entity Registry*
a digital certificate authority that is supported by a standards-based interface and supporting the messaging framework and trust framework	
a standards-based interface to a directory of all entities participating in exchange	*Entity Registry* and *Service Registry*
a directory of entities participating in exchange	
a standards-based interface to a directory of providers participating in exchange	*Service Registry*
a directory of providers participating in exchange	
a standards-based service specification for discovering patient identities and agree on shared identities	*Patient Discovery Specification*
a standards-based service specification for (1) a push exchange pattern, (2) a query and response exchange pattern, and (3) a publish and subscribe exchange pattern	*Query and Response Exchange* and *Information Submission Specifications*

Meaningful Use Requirement	Infrastructure Component
a gateway interface to the Nationwide Health Information Network	*NHIN Gateway*

Figure 5 illustrates the architecture for the State Infrastructure, and its relationship to stakeholders, including Entities, Nodes, and individuals.

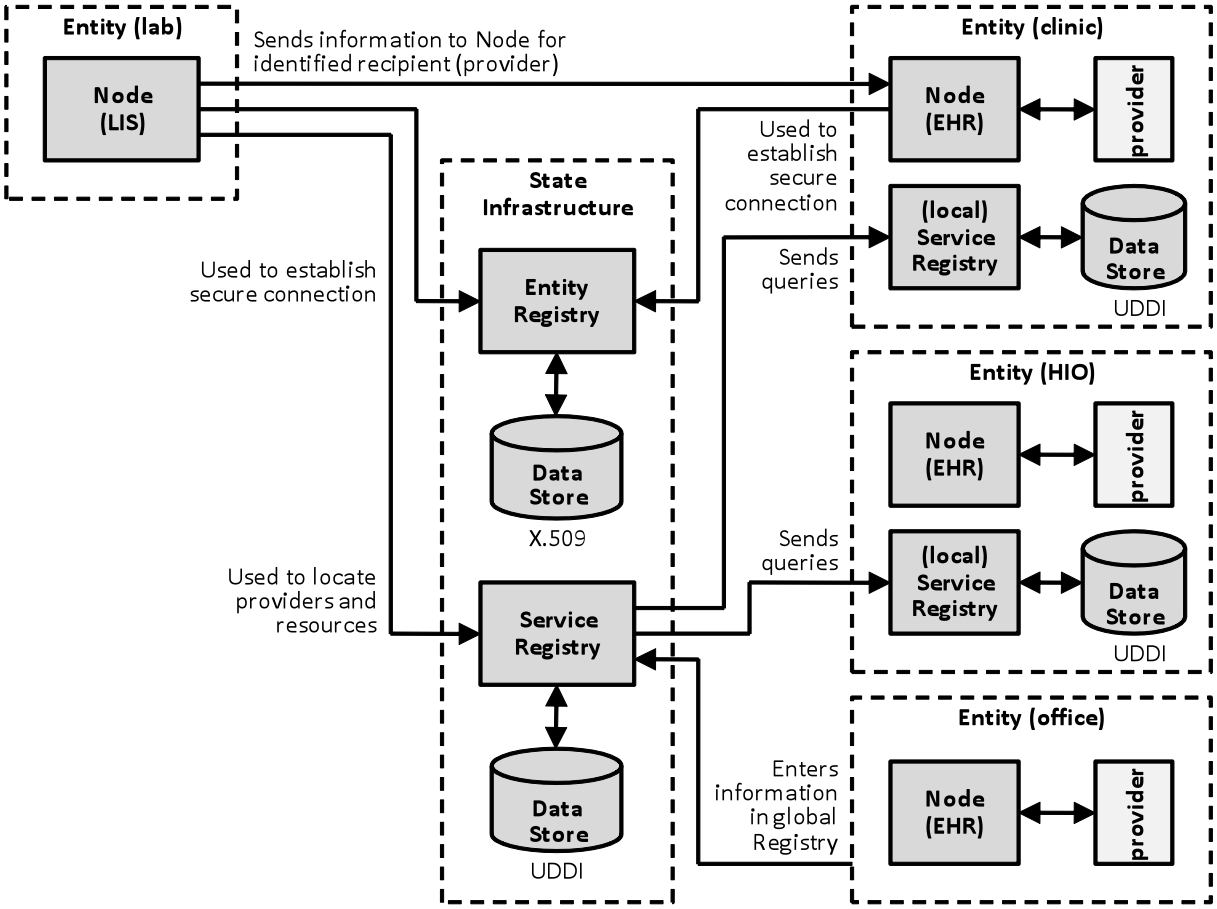

Figure 5 High-level architectural diagram of the State Infrastructure, including Entities, Nodes, providers, and patients, to illustrate their relationships and interactions.

In this diagram, the major State Infrastructure components are illustrated for the Entity Registry and global Service Registry, as well as the local Entity Registries of some Entities that wish to manage their own UDDI registries. It only illustrates an Information Submission interaction between two organizations – other interactions are supported by the same components, and interactions can be with multiple organizations. The illustration also identifies only clinical Entities and EHRs as Nodes as possible recipients of information. All valid Entities should be represented, and the diagram has not indicated these additional stakeholders for simplicity only.

Like the illustration in Figure 1, Figure 5 shows how a lab (an Entity) can use its lab information system (a Node) to send a structured lab result to the EHR (another Node) used by a specific provider identified in the lab order at his/her clinic (an Entity). To do this, it:

1) uses the Service Registry to identify a web service address for the recipient provider's EHR and a definition of the protocol used to send information to it, potentially using the global Service Registry to orchestrate a search across all Entities including those with local Service Registries or contacting the local Service Registry of a known Entity directly;
2) uses the Entity Registry to create a secure, encrypted, reliable, and validated connection to the EHR using certificates for the LIS and EHR Nodes;
3) attests to the authorization for the exchange on behalf of the lab official responsible for the result[3] using its Entity certificate, which is validated by the EHR Node; and
4) uses a standards-based service to exchange the information.

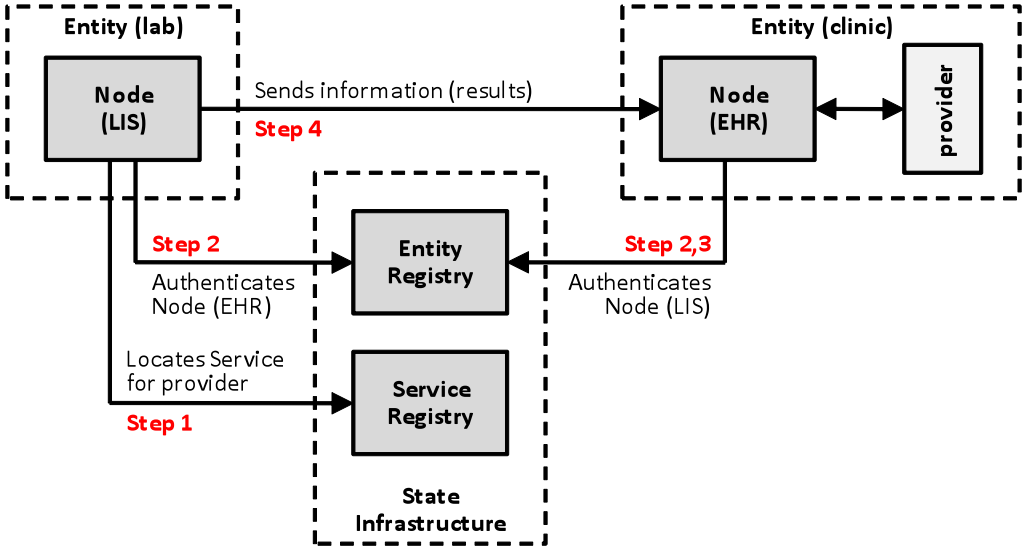

Figure 6 High-level view of how the State Infrastructure is used to transmit structured lab results from a lab system to a provider's EHR.

Again, the lab system takes responsibility for creating structured lab result content. The State takes responsibility for the Service Registry used to locate the provider's EHR and define the web service interaction. The State also takes responsibility for the Entity Registry used by the lab system and EHR to establish a secure, encrypted connection. The provider's HIO or EHR vendor takes responsibility for incorporating the structured lab result content into the EHR.

3 Note that laboratories are required by regulation to identify an individual that takes responsibility for lab results. The structure of the Authorization Framework and Entity Registry allows for that requirement to be fulfilled.

4 Discovery and Exchange Service Specifications

In addition to the key infrastructure specifications for the Messaging Framework and Authorization Framework, the architecture should provide for at least one specification to support patient discovery and each of the exchange patterns required for meaningful use. These specifications should include:

- *Patient Discovery Specification(s)*: Standards-based mechanism(s) for two entities to agree that a match exists for a patient within each entity based on the exchange of demographics allowed by State policy and local policy of the entity. The Patient Discovery mechanism(s) should conform to the Messaging Framework and Authorization Framework, and should not require the use of a statewide identifier or statewide MPI.
- *Query and Response Exchange Specification(s)*: Standards-based mechanism(s) for one entity to request health information from another and retrieve that information, conforming to requirements of the Messaging Framework and Authorization Framework, and perhaps dependent upon Patient Discovery to enable patient matching.
- *Information Submission Specification(s)*: Standards-based mechanism(s) for one entity to submit health information to another without the explicit requirement for an electronic request, conforming to the requirements of the Messaging Framework and Authorization Framework.

The State Infrastructure supports the development and support for multiple specifications for Patient Discovery, Query and Response Exchange, and Information Submission, based on the needs and available standards. For example, the Service Registry may return multiple web service addresses supporting multiple protocols for the delivery of lab results information for a single provider and single EHR Node. The lab vendor may choose among them for the service most appropriate for the exchange at hand.

This approach to development – one in which multiple protocols and services may support a single type of exchange – promotes industry innovation. It does, however, contribute to standards proliferation, and must be appropriately managed.

An example specification for Patient Discovery, Query and Response Exchange, and Information Submission follows, based on the NHIN Exchange web service specifications.

4.1.1 Patient Discovery

Patient Discovery provides the ability for one Entity to determine whether other Entities have records for a given patient by submitting a set of demographic identifiers that can be used to match against their own master patient indices.

The Patient Discovery service specification might be based on the IHE profile for Cross-Community Patient Discovery (XCPD). The actions of XCPD are illustrated in Figure 7 below. XCPD is an arbitrated conversation between two Entities, in which a querying Entity submits a query to one or more others with its patient ID and demographic information about the patient as it is known to it. Queried entities search their patient indexes for matches. If a match is found, and sharing that patient ID with the other Entities is allowed by policy and patient consent, it sends its patient ID and the demographic information as it is known to it back to the querying Entity. A match is declared if and only if both Entities agree on the match.

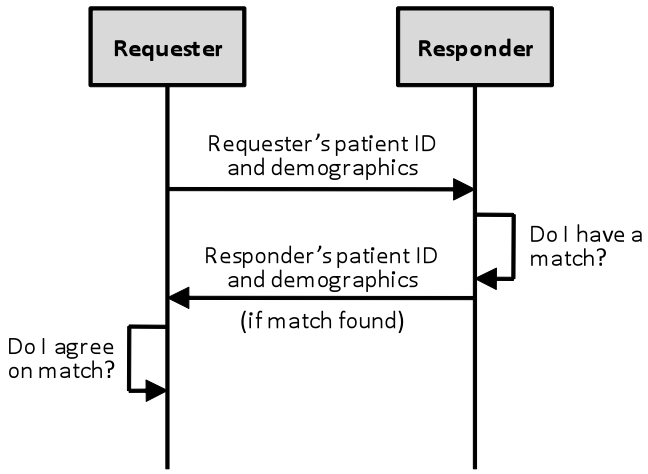

Figure 7 Illustration of a suggested model for a Service Specification for Patient Discovery.

When queried for a match, an Entity might return one of a number of responses:

1) success, in the form of a patient ID and demographics;
2) success with multiple matches, in the form of a list of patient IDs and corresponding demographics;
3) potential success, in the case of an ambiguous match which might be resolved with additional information to produce a single matching patient; or
4) no match, which might might result from a failure to identify any matches, an ambiguous match when policy prohibits a request for additional information, or a failure to meet the authorization requirements of policy or patient consent even if a match is found.

Policy must determine whether a response with multiple matches or a request for additional information in the case of an ambiguous match are allowed. Cal eConnect should take a role in determining State policy, which may be further constrained by local policy in line with concept of local autonomy.

Importantly, XCPD is a conversation between two Entities to reach an agreement on a matching patient. In order for there to be a match, and for exchange to proceed, both Entities must agree that the patient is a match, even if they utilize different matching rules internally. XCPD does not require any centralized master patient index or any national identifier. It also requires no centralized service in order to arrive at matches, but is a specification for how two or more entities would arrive at a match.

4.1.2 Query and Response Exchange

The Query and Response Exchange pattern might be based the IHE profile for Cross Gateway Query (XCA). XCA achieves exchange through a two-step process implemented as two separate services: a query operation followed optionally by one or more retrieve operations.

XCA-based query allows one Entity to locate health information associated with a specific patient. An Entity might use Patient Discovery to learn the patient ID of the patient. A query returns a list of documents for a given patient based on a set of search criteria. XCA-based

retrieval allows an Entity to retrieve documents from the list returned by a query. Retrieval is optional; if no document of interest is returned via a query, no document needs to be retrieved.

The XCA specification was relaxed within NHIN Exchange to support the query for, and retrieval of, dynamically generated document content. Cal eConnect should consider a similar strategy to allow Entities to manage health information in any form they desire internally.

XCA is also inherently document-based. NHIN Exchange utilizes clinical document architecture (CDA) documents based on the HL7 version 3 standard. Cal eConnect might further relax the specification to allow exchange of the various payloads included in the IFR to support various meaningful use criteria.

Figure 8 illustrates the XCA exchange pattern. XCA requires the unique patient identifier of the Entity providing the data. As a result, it is likely preceded by Patient Discovery, not shown in Figure 8, but the patient identifier can be obtained by other means.

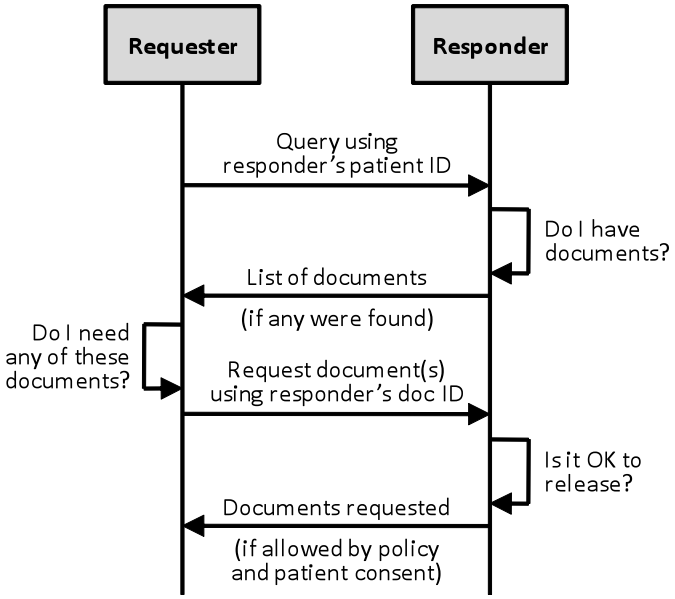

Figure 8 Illustration of a suggested model for a Service Specification for Query and Response Exchange.

In this context, a "document" refers to the form of electronic health information as it is transferred between Entities not as it is stored within systems such as EHRs in that entity. Entities that generate documents dynamically on demand may be required to ensure that the generated document remains available, unaltered, once a document has been retrieved once. This means that Entities or systems that generate dynamic documents must retain those documents for some period of time. Cal eConnect should determine the policies associated with dynamic documents that might include that they be stored by the Entity that generated them rather than generated dynamically a second time if requested.

4.1.3 Information Submission

The Information Submission service allows an Entity to send information to another without a corresponding electronic request. The transactions implemented by the Informatino Submission

service specification might be based on the IHE profile for Cross-Enterprise Document Reliable Interchange (XDR).

XDR provides the ability for one Entity to "push" identified health information for a given patient to another, triggered by events at the initiating Entity. It might be used, for example, to deliver lab results electronically when the order was received by paper, or to submit quality measures on a prescribed schedule. This unsolicited submission of information is the most common exchange pattern required by the meaningful use criteria, and the only one being developed by NHIN Direct.

Figure 9 illustrates the simple push transaction implemented by XDR.

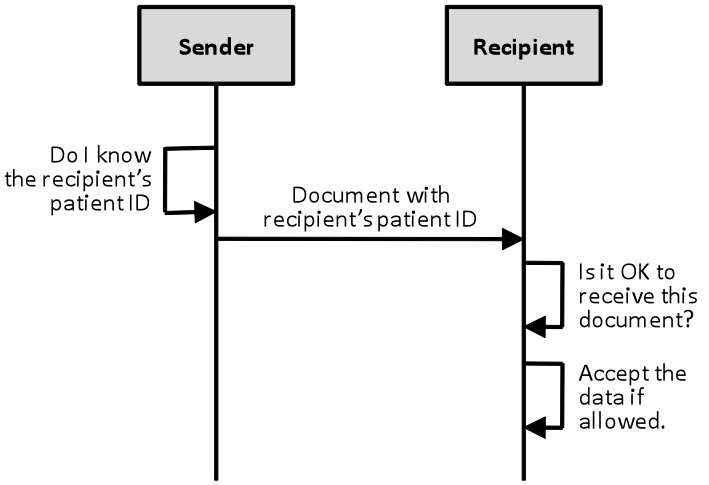

Figure 9 Illustration of a suggested model for a Service Specification for Information Submission.

XDR normally requires that the patient identifier of the receiving Entity be know, and therefore XDR may be used in conjunction with Patient Discovery to retrieve the patient ID of a matching patient. It may also be used without Patient Discovery when the patient identifier is known by other means. For example, a lab order may include identifying information that allows a lab to send results via XDR with a patient identifier without the need for Patient Discovery.

4.1.4 Information Feed

NHIN Exchange identified a need for and includes a publish and subscribe mechanism based on the W3C standards for WS-BaseNotify and WS-Topics. However, an analysis of meaningful use criteria suggested that only one criteria – syndromic surveillance – would make use of information feeds, and that need could be provided using Information Submission as well.

Cal eConnect should determine, in collaboration which public health and other stakeholders, whether it is necessary to develop and promote a Service Specification for information feeds, perhaps based on the NHIN model for publish and subscribe.

4.1.5 Implementation Strategy

In its work supporting the Operational Plan, the California eHealth Technical Working Group (TWG) recommended that the State develop and adopt a small set of exchange specifications that the State encourages, or perhaps requires, all participating Entities and Nodes to support.

Based on the requirements for meaningful use, this would include specifications for Patient Discovery, Query and Response Exchange, and Information Submission. It is also recommended that the State allow additional standards-based discovery and exchange patterns between organizations, as long as they conform to State policies, in order to foster innovation and enable new Business Services.

Cal eConnect should first determine whether it will establish and require a minimum set of exchange services be supported by each Entity. The advantage is that it establishes a lowest common denominator for all exchange partners, while allowing for more efficient or emerging patterns if both partners support them. However, it raises the bar for participation.

In any case, Cal eConnect should take responsibility reviewing, approving, and cataloging specifications that conform to State Infrastructure and policy requirements and may be listed in the Service Registry. This could be accomplished through a process similar to that outlined in Section 3.1.4 for the implementation of the Messaging Framework and Authorization Framework. If that approach is taken, it is recommended that examples be taken from NHIN Exchange, IHE, and/or Council for Affordable Quality Healthcare (CAQH) CORE Phase I and Phase II as a basis, with minimal customization to reduce the time required for development and maximize the likelihood of industry vendor support.

Alternatively, Cal eConnect could develop a set of approved discovery and exchange specifications by allowing individuals, stakeholders, SDOs, industry organizations, or vendors to submit candidate standards to a review board for public comment and review. The latter approach is recommended, as it allow Cal eConnect to focus on State Infrastructure. The Internet Engineering Task Force (IETF) successfully uses such a model to develop international standards for the Internet.

Independent of the approach, the development of specifications must be preceded by definition of the policies that define privacy and security, and the role and process for patient consent, as well as development of the Messaging Framework and Authorization Framework specifications.

4.1.6 Resource Requirements

If Cal eConnect chooses to follow option one and develop specifications itself, the effort should be managed part time by a CTO or Systems Architect on staff with Cal eConnect (perhaps 50% effort) over a 3- to 6-month period, utilizing one shared full-time staff facilitator to manage workgroup(s) comprising volunteers from the community and one technical writer or consultant for each specification to draft the specifications and collect and review public comments.

If Cal eConnect chooses to follow option two and review candidate specifications submitted by the community, it would require part-time oversight by a CTO (perhaps 20% effort) and a half-time Systems Engineer or consultant with health IT expertise during the review process for each specification, plus monthly meetings of a Change Review Board comprising stakeholder representatives identified by Cal eConnect to review analysis and make recommendations.

The process will require the use of web sites to publish drafts and collect comments (perhaps using a wiki or other Web 2.0 mechanism), and web-based meetings to facilitate the workgroups or review boards.

5 Business Services

Business Services comprise a set of value-added software components and their service-oriented interfaces available to any eligible stakeholder in the California health care system. They are built upon and use the State Infrastructure. The purpose of these services is to enable value-added, complex business processes, perhaps by orchestrating complex interactions on behalf of an Entity or individual. Business Services may be

a) governed, developed, and operated by by Cal eConnect, or
b) may be developed, operated, and offered by third parties as a busienss under Cal eConnect governance.

The analysis of meaningful use identified a number of high-level value-added services as candidates for Business Services. Table 4 below outlines some of the value-added services from that analysis.

Table 4 Summary of high-level value-added services that are not required for meaningful use, but might have value to stakeholders.

Meaningful Use Criteria	Potential Value-added Functionality
• Lab results delivery • Public health reporting • Public health surveillance	Translation service that facilitates translating structured lab results into standard format(s)
	Lab services as a single delivery point for lab systems that facilitates routing of lab results to appropriate provider systems and/or public health departments
• Eligibility verification	Lab services as a single access point for EHRs and practice management systems for insurance eligibility information via EDI transactions across various health plans
• Provide copies to patients • Provide patient access	Widespread secure messaging system to enable patients and providers to communicate electronically.
• Exchange among providers • Summary at care transition	Translation service that facilitates translating and transforming among standardized summary clinical formats.
	Lab services as a single delivery point for EHRs for routing clinical summary documents among providers and patient-designated entities.
• Submit immunizations	Lab services as a delivery point that can accept immunization messages from EHRs and forward them to the intended immunization registry.
• Public health reporting • Public health surveillance	Utility service to manage pseudonymization and re-identification when required.

The California eHealth Technical Advisory Committee (TAC) prioritized the development of Lab Services as a value-added Business Service for consideration. The Lab Services is used as an illustration of the system architecture for Business Services.

5.1 Lab Services

The potential activities of the Lab Services are outlined in Section 2.2 *Example Illustrating Portions of the Architecture* as an example of how a Business Service interacts with the State Infrastructure. A more detailed description of the potential Service or its inner workings is not included here. Instead, the externally-visible characteristics of the Service and its interactions with Infrastructure components is described, as an example of the architecture for any Business Service.

Figure 10 illustrates how the Lab Services fits into the State Infrastructure, and how it interacts with Entities and Nodes.

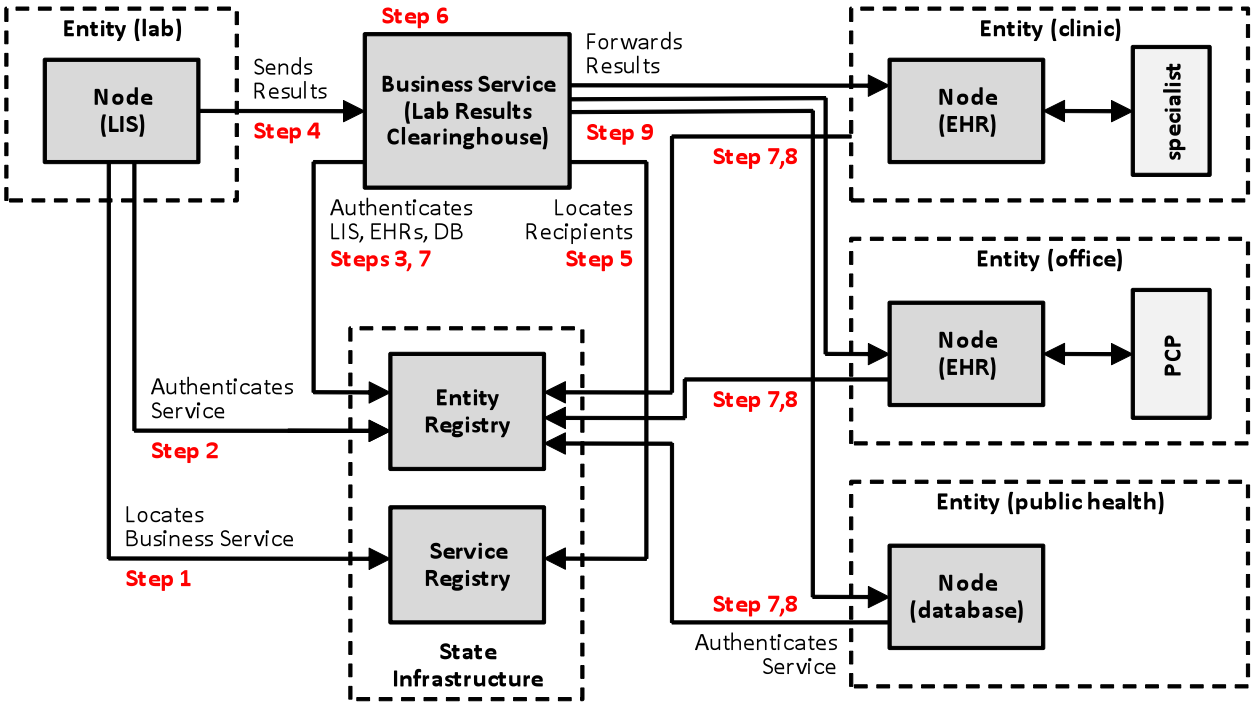

Figure 10 High-level view of a potential architecture for the Lab Services and its interaction with State Infrastructure, labs, and recipients of lab results.

All Business Services must conform to the Messaging Framework and Authorization Framework. The organization providing the Business Service is provided an entry in the Entity Registry and a digital certificate with which to sign authorizations. The Service itself is provided a Node entry in the Entity Registry and a digital certificate to use in establishing secure, encrypted, reliable connections on the Internet.

The Business Service is also provided an entry in the Service Registry, describing the Business Service, the address of the web service it implements, and the protocol to use in accessing it.

Cal eConnect manages entries in the Entity Registry and monitors activities of the organization providing the Business Service, if not Cal eConnect, in order to ensure its operation in compliance with State policy. If violated, entries are removed from the Entity Registry and certificates revoked.

The Business Service contains and implements all orchestrated interactions with the State Infrastructure and Nodes within the statewide exchange. It may store PHI or other information if allowed by State policy. If a Business Service needs to create a connection with a Node or other Business Service, it uses the Service Registry to locate the address and protocol for the web service for that Node, and the Entity Registry to access the digital certificates necessary to establish a secure connection.

In this illustration in Figure 10, the lab:

1) uses the Service Registry to identify a web service address for the Lab Services and a definition of the protocol used to send information to it;
2) uses Node certificates in the Entity Registry to create a secure, encrypted, and validated connection to the Lab Services;
3) asserts authorization for the exchange using its Entity certificate in the Entity Registry, which is validated by the Lab Services; and
4) uses a standards-based service to exchange the information – perhaps one identified by a mandatory Exchange Service Specification or perhaps one specific to the Business Service.

The Lab Services in turn:

5) uses information sent to it by the lab and rules provided by public health agencies to determine a list of recipients, in this example a specialist ordering the lab, the primary care physician that referred the patient to the specialist, and a public health surveillance systems, and then uses the Service Registry to identify
    a) a web service address for the specialist provider's EHR and a definition of the protocol used to send information to it,
    b) a web service address for the primary care physician's EHR and a definition of the protocol used to send information to it, which may be different, and
    c) a web service address for the public health reporting and surveillance system and a definition of the protocol used to send information to it
6) translates the structured lab result into the terminology used by each system and transforms the format into the standard used by each system, again all of which may be different, and removes identifying information from the message bound for the public health system, if required;
7) uses the Entity Registry to create secure, encrypted, and validated connections to both EHRs and the public health system in turn;
8) asserts authorization for each exchange in turn using its Entity certificate in the Entity Registry, which is validated by both EHRs and the public health reporting and surveillance system; and
9) uses standards-based services to exchange the information with each system, in turn; perhaps using services identified by mandatory Exchange Service Specification.

The suggested architecture illustrated in Figure 10 is only one possible solution for the Business Service. However, it illustrates how the Service makes use of State Infrastructure components. Use of Business Services is strictly voluntary.

5.1.1 Implementation Strategy

Cal eConnect might select from a number of potential implementation methods for Business Services in general, including the Lab Services.

1) Cal eConnect could choose to issue a grant to a local HIO that has developed a similar capability to the Lab Services so that it can expand the capability, ensure its compliance with the State Infrastructure, and offer the Business Service statewide. The grant would have to outline the business relationship with the HIO, operating responsibilities, and revenue-sharing, based on the level of expansion and grant support required by the HIO. If a solution is available in an existing HIO, this may provide the mostly timely mechanism to offer the Service statewide.

   It is believed that there exist HIO capabilities within California that could utilize this option.

2) Cal eConnect could conduct a competitive procurement to contract with a vendor, software developer, and/or systems integrator to create Lab Services that it delivers to Cal eConnect to operate. This option perhaps holds the highest potential for revenue generation for Cal eConnect, but requires the highest initial investment.

   There exist several HIE vendors that have the capability to develop generalized Lab Services based on their current technical capabilities and may be able to provide it at the scale required for the State. In addition, Quest Diagnostics has a lab results reporting hub that might be made available to the State, if it can successfully incorporate data from other labs in its solution.

3) Cal eConnect could hire a development staff, and develop and maintain the Lab Services as a core competence and part of its business model. This option has investment requirements and revenue potential similar to the procurement route, but requires a longer-term commitment on the part of Cal eConnect to create, manage, and operate a business that develops software. HIOs within the State may also see this approach directly competing with their capabilities and business models.

   While there exist developers with the requisite skills, there is some risk associated with creating a successful development team rapidly. This approach requires strong technical and management leadership on staff with Cal eConnect.

4) Cal eConnect might solicit submission of business models from vendors, HIOs, or other organizations that would develop the Lab Services or other Business Services not even contemplated by Cal eCnnect, and operate the Service as a business. Cal eConnect's role would be governance and monitoring of the Service to ensure that it conforms to State policies. This approach minimizes both the investment and the revenue potential, but fosters innovation and most rapidly develops a broad collection of capabilities.

   There well may be businesses and/or HIOs interested in making the internal investment to create a Business Service compliant with the State Infrastructure requirements in return for access to the State market for a small access fee.

The choice of implementation approach is primarily dependent upon the role Cal eConnect sees for itself in creation of Business Services: grantor, buyer and operator, developer and operator, or facilitator.

5.1.2 Resource Requirements

The resource requirements for the Lab Services is completely dependent upon the desired functionality and the implementation strategy Cal eConnect and business model selects.

1) If implemented through a grant, the size of the investment would be less than that to develop the service from scratch. The revenue potential would be dependent upon the business relationship called for in the grant.
2) If procured through a vendor, the Service would require significantly more investment to create and would most likely require continuing license fees to operate, especially if based on an existing vendor solution. If developed from scratch, the service might require on the order of $2-5 million to develop, depending upon the complexity of the standards for structured lab information it supports. Higher development and maintenance costs would be required if terminology translation is included in the offering.
3) If developed through Cal eConnect staff, the Service would likely require slightly more investment to create rather than procure the capability due to the lack of efficiency of a new development shop, and might still require ongoing license fees unless the solution was based entirely on open-source software.
4) If solicited as a business to be run by a third-party, the investment would likely be limited to oversight of the review, contracting, and monitoring process.

All activities involving Business Services should be overseen by a CTO or Systems Architect and a security specialist on staff with Cal eConnect, and use the facilities of a monthly Change Control Board.